Computer Security Investment Strategy, FY 1985-91 (U)

November 1984

Copy 024

Computer Security Investment Strategy, FY 1985-91 (U)

Prepared by the Computer Security Working Group, Information Systems Board. (U)

Computer Security Investment Strategy, FY 1985-91 (U)

Key Judgments

The working group reached a number of conclusions regarding information systems and network security in the Agency:

- Future technologies, particularly the growth of desktop computers, the increased local storage of data, and widespread networking, will exacerbate existing security vulnerabilities as well as create new ones.
- A considerable body of knowledge and technology exists today that could be used to improve the security of existing information handling systems and networks.
- The explosion of technology within the Agency means that the vulnerabilities of our information handling systems are actually increasing.
- We now depend heavily on procedural and personnel security as well as physical isolation to protect our electronic information handling systems. Within 10 years these measures will no longer be an adequate shield.
- The present gap between available security technology and installed safeguards will significantly widen unless security standards are firmly coupled to the new information handling strategies.
- The proper use of the new information and communications security tools requires a comprehensible set of data protection policies, standards, and requirements.
- Information systems security education and training will become increasingly important as the majority of our people become computer literate.
- Because of the constantly changing nature of both the technology and the threat, modification of this strategy will be required continually.

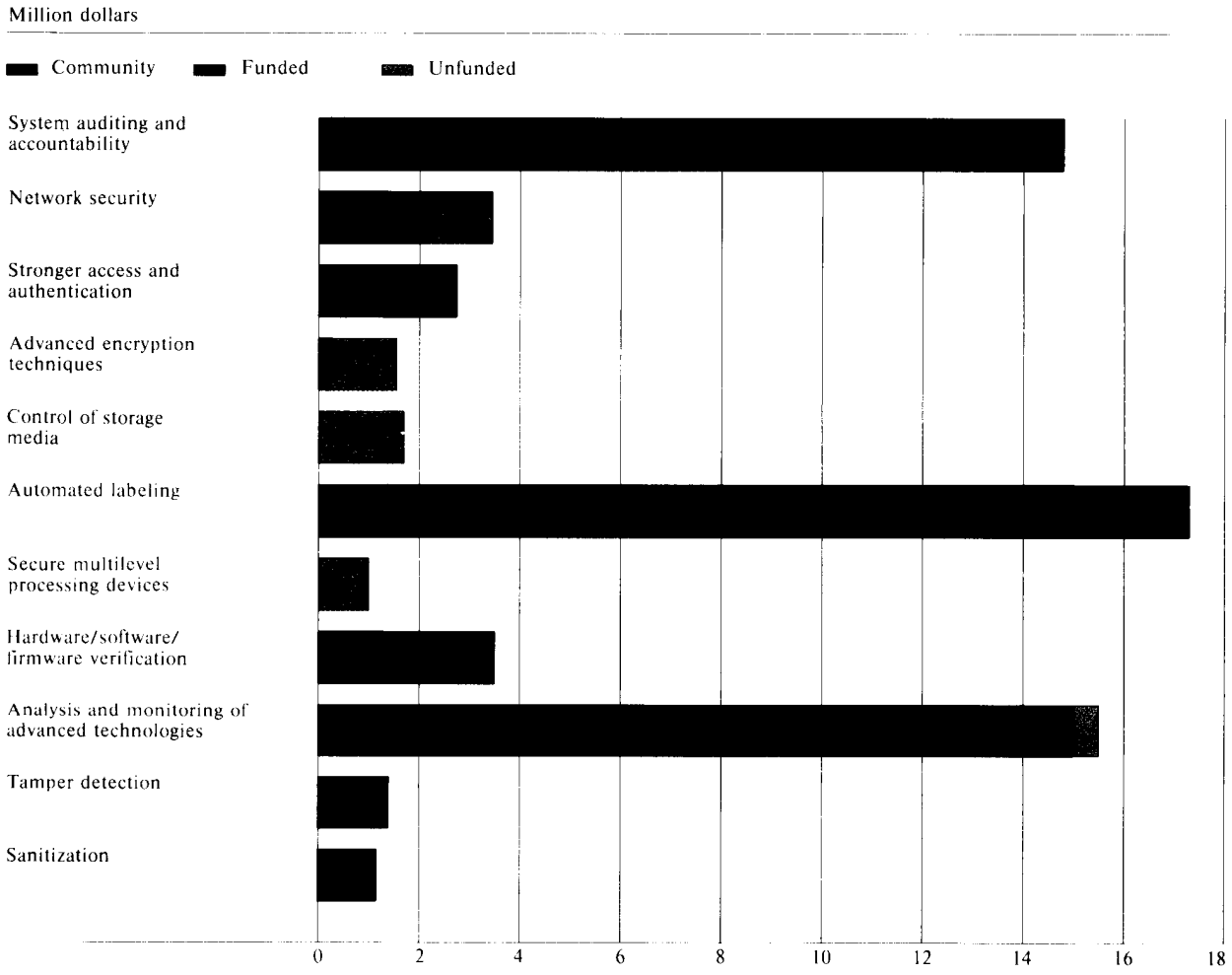
The following initiatives, discussed in detail in the report, should be funded:

— System Auditing and Accountability.
— Network Security.
— Stronger Access and Authentication Controls.
— Advanced Encryption Techniques.
— Control of Storage Media.
— Automated Labeling.
— Secure Multilevel Processing Devices.
— Hardware/Software/Firmware Verification.
— Analysis and Monitoring of Advanced Technologies.
— Tamper Detection.
— Sanitization.

This information is Confidential.

Contents

Recommended Expenditures for Information Systems Security, FY 1985-91



25X1

304157 11-84

Computer Security Investment Strategy, FY 1985-91 (U)

Introduction

In May 1984 the then Executive Director, Charles Briggs, requested an investment strategy for improving the security of information in automated environments. This report proposes a strategy for attacking information systems and networks problems that we know exist today, and those that we believe will emerge as a byproduct of new technology. 25X1

Given the increasing competition for Agency resources, we offer this report to the Executive Committee as a means of evaluating this combined information systems and networks security program throughout the budget process. 25X1

Despite an unprecedented commitment to the automation of the Agency's information handling systems, even greater effort will be required to cope with the vast increases in information the CIA will process, analyze, report, and systematically store and retrieve in the next decade. For example, Cable Dissemination System traffic has more than tripled since 1976 and could well triple again by the late 1980s. DO traffic alone, which has more than doubled since 1976, is now increasing by 20 percent a year. New collection systems are expected to double or triple the information available from those sources by 1990. 25X1

Recognizing that the security and integrity of information systems and communications links will be an overriding priority in their future development, the Executive Director called for an amendment to the Agency's 1982-92 Strategic Plan. He wrote that this blueprint should address "several areas in which CIA's needs are so urgent that we must set the pace in research, development, and applications. Computer security is one of these areas."[1] 25X1

In developing the report, we first created a view of the Agency's automated information handling environment in 1992, discussing the most serious present and future problems of information systems and networks. 25X1

Against this backdrop, we solicited the office strategies of individual line organizations, such as Security (OS), Communications (OC), Data Processing (ODP), and Research and Development (ORD), to resolve these shortfalls 25X1

The working group ranked these individual office initiatives into a primary group of five that we believe must be accomplished, and a secondary group of six that should be vigorously protected. 25X1

We have rank ordered the initiatives so that the most serious issues are addressed first, and we have also loaded individual initiatives at the front end so that they can be accomplished as quickly as possible. 25X1

[1] From *Addendum (1984)* to the Central Intelligence Agency Strategic Plan, 1982-92 25X1

The FY 1985 cost at the recommended spending level is $5.8 million; the total cost through FY 1991 is $66 million. Some 56 percent of this FY 1985 amount is already reflected in existing office and COMPUSEC budget requests so that the funds not already requested total $2.55 million in FY 1985. Surge funding and low-guidance figures for each program are also provided. Overlap with DOD Computer Security Center and COMPUSEC efforts has been avoided by taking advantage of their activities wherever possible. 25X1

The need for information security exists in literally every facet of Agency operations, and its perceived shortcomings and potential impact is a topic of considerable interest. Accordingly, discussion and coordination of this report were held within the Agency and the Intelligence Community in order to avoid gaps, duplication, and overlap of efforts. This plan is a basic, high-level strategy rather than a comprehensive blueprint. 25X1

The DOD Computer Security Center is doing basic research on many pressing issues in the field of information systems and networks. Interested Agency elements routinely trade concerns, experiences, and information on research initiatives with the Center as well as with other security units. We have attempted to ensure, therefore, that the programs described in this report do not compete with efforts going on elsewhere in the Community but rather address the Agency's unique concerns. 25X1

Likewise, computer vendors are reacting to the growing awareness of and concern about information systems security. Their efforts were also factored into this strategy. 25X1

Environment and Vulnerabilities

Four major environmental trends are emerging:

- Our increasing dependence on computers.
- Our acceptance of personal computers (PCs).
- The increased use of packaged software.
- The growth of integrated Agency information handling networks. 25X1

PCs are being accepted at a faster rate than was the telephone. This explosive growth is largely due to the usefulness of the computer in providing sophisticated word processing, electronic mail, access to cable traffic, and other forms of communication such as video and audio. 25X1

The development of complex but user-friendly packaged software tools for PCs as well as mainframes will increase the usefulness of ADP to Agency employees. Because of the ease with which new capabilities can then be implemented, nearly all employees will be using some form of workstation that capitalizes on advanced capabilities such as graphics, data base management systems, and spreadsheet capabilities. As a result, the volume of information stored on Agency computers will increase by several orders of magnitude. 25X1

Out of the need to share information worldwide and to support critical Intelligence Community operations, existing networks will expand, often interconnecting, to form a vast integrated Agency Information Handling Network comprising many independent yet connected subnets. These networks, characterized by high speeds and huge throughput, will be used for far more than message communication; they will allow the transfer of large data files as well as carry voice and video signals.

25X1

Out of this environment come new threats. Sophisticated software offers broader exposure to trapdoors and trojan horses, which can allow unauthorized access. Compact, high-density storage media are easy targets for theft or misuse. The availability of powerful and convenient lap-top and hand-held devices will bypass present access, authentication, and control procedures. Networks will dramatically increase the potential for unauthorized access and also create complex multilevel security issues when computers, indeed networks, operating at one security level connect with computers operating at a different level. Moreover, the aggregate of information that can be extracted from a vast information-sharing network will pose an additional threat not present in a single computer system.

25X1

Today, the CIA relies heavily on procedural and personnel security to protect against unauthorized access and spillage. It also relies on limited automated access controls and auditing features for maintaining compartments of information and for enforcing need-to-know. Such safeguards, however, are becoming overly taxed for several reasons. In a world of information-sharing and dial-up capabilities, strict physical control of the total number of persons with access to information will not be feasible. We must have security features embedded within our systems. Also, the automated access controls and other security features that do exist within our systems have typically been patched onto systems and cannot be trusted to function without some gaps or failures. Furthermore, these security features have been designed for single computer systems, not networks; networks present far more complex challenges than do single computer systems.

25X1

The environment, associated risks, and safeguards currently in place are defined in detail in the appendixes.

25X1

The Strategy

The future operating environment and the threats and vulnerabilities inherent in that environment form the basis of our strategy to provide improved computer security.

25X1

As a strategic goal, computer security must counter threats, reduce known vulnerabilities, and identify and initiate responses to future emerging vulnerabilities. Our strategy is to invest in those initiatives that best meet the following criteria:

- Ensure that future systems surpass the security protection of current systems.
- Automate more security functions to augment the human process.
- Include security as an integral part of future Agency systems rather than retrofit security to systems as an afterthought.

- Pursue the development of network security across Agency, Community, and government boundaries.
- Centralize access controls and auditing functions where feasible.
- Emphasize those threats or vulnerabilities that require an immediate response.
- Use commercially available, vendor-supported products to maximize and accelerate accomplishment of security goals when possible.
- Design security systems that can adapt quickly to changing conditions and that will not be made obsolete by minor changes in a threat or vulnerability. 25X1

Recommendations

Given this automated environment of 1992 and the threats associated with this environment, the working group recommends the following programs and policy initiatives that address the most serious present and future problems of information systems and networks 25X1

Technical Initiatives

This section contains 11 specific initiatives where additional money and personnel are required:

- Initiatives 1 through 5 are vital to the success of the strategy.
- Items 6 through 11 should be vigorously protected if we intend to operate our systems at their full capacity and capability. 25X1

1. System Auditing and Accountability. Computer security audits are being used today as the basis for detecting abnormal system activities (such as unauthorized attempts to access files) and to signal the occurrence of any unusual or potentially hostile activity. This program is still maturing—the present checks require extensive manual reviews of numerous printouts to detect problems. A program to significantly automate this auditing and accountability on Agency systems requires the requested funds to implement this initiative. 25X1

The Agency has no real-time audit capability at present because these checks are routinely done a minimum of 24 hours after the fact. This program will develop auditing tools that will isolate and thus allow us to neutralize problems as they arise and before serious damage can result 25X1

The program began in FY 1983 using reprogramed funds. It has been included in the FY 1985 COMPUSEC initiative as an Intelligence Community effort. See appendix A for additional details and specific dollar and personnel costs. 25X1

2. Network Security. Agency participation in Community data-sharing initiatives has been identified as a long-term strategic goal. Trusted networks, however, do not exist on an IC-wide basis today. Nor can they be shared in the same overseas locations or interoperate during emergencies. Multilevel secure networks that can support this national objective of commonality and survivability by allowing separately managed systems to intercommunicate securely via gateways must be developed. 25X1

Although these networks evolve out of the union of communications and computers, their security issues are more than the simple union of the security issues of communications and computers. The problems in both areas combine, and new problems emerge from the interactions between multiple computers and communications lines. These are problems that are unique to networks or of greater complexity in a network environment. 25X1

Some work is being done on secure local area networks and office automation systems. The general problem of network security is not being addressed, however. 25X1

Network security is a COMSEC initiative due for initial funding in FY 1985. See appendix A for details. 25X1

3. Stronger Access and Authentication Controls. Agency users of automated information handling systems gain access today by simply matching their unclassified userid with a classified password. Although the secrecy of this password provides a measure of access controls, experience shows that this method is far from fail-safe. Indeed, there have already been a number of security incidents directly attributable to password abuse. 25X1

With our rapidly expanding user community, the strengthening of access controls is becoming increasingly important. There must be a greater emphasis on the authentication and verification of each individual's access, particularly for users located away from Headquarters 25X1

As the Agency moves toward automation, many of the administrative and management controls of our paper offices will be replaced with their electronic equivalents, but without the human controls that allow these systems to operate today. The release of cables and the signing of vouchers are but two examples of areas where more positive identification and authentication at the terminal will be required. 25X1

This program will also ensure that the functions of control sheets, registries, and couriers we use today to control the flow of data are duplicated in an electronic environment. 25X1

The program began in FY 1983 using reprogramed funds. It has been included in the FY 1985 COMPUSEC initiative as an Intelligence Community effort. See appendix A 25X1

4. Advanced Encryption Techniques. Continued development is needed for at least three new types of encryption to serve applications other than the traditional communications link protection. These are "end-to-end," file, and data base encryption. 25X1

End-to-end encryption will provide unbroken security protection between individual terminals and users rather than between clusters of devices fed into a single crypto box as is commonly done today. File encryption will provide privacy and compartmentation in a "system high" environment where all users of the system could normally have access to volumes or files. Data base encryption will protect national security information stored on disks in facilities that are subject to hostile overrun or theft. None of these three encryption applications are receiving adequate attention at the present. 25X1

*5. **Control of Data Storage Media.*** Data must be protected from unauthorized or accidental disclosure while it resides on various storage media such as magnetic tape, rigid disk, and flexible disk. Control methods used elsewhere, such as tagging clothing in stores, will be explored as a means to detect attempts to remove the media from authorized areas. New technical labeling methods will also be investigated to prevent the accidental mishandling of media. The project will not be limited to magnetic media; as new technologies of data storage media come into use, they will be included. 25X1

Previous efforts in this area have not yet produced a solution to the problem. A new look, which is closely linked to physical and procedural security measures, is recommended 25X1

This project is not yet funded. 25X1

*6. **Automated Labeling.*** At present there is no automated way to match the classification of a data element to a potential recipient's clearances and access authorizations 25X1

Automated labeling will allow electronic sharing of data by comparing the data's sensitivity controls (that is, classification caveats and discretionary labels such as "Exclusive For" and "Orcon") with the potential recipients' access authorization. 25X1

Automated labeling is a COMPUSEC initiative due for initial funding in FY 1985. 25X1

*7. **Secure Multilevel Processing.*** The inability to enforce data separation by classification level and compartments as well as according to control restrictions such as Orcon and Exclusive For is a major shortcoming in today's intelligence processing environment. 25X1

Because the majority of vendor-supplied hardware and software is inadequate for our security requirements, CIA computer centers operate in an environment in which strict compartmentation and need-to-know is impossible to guarantee. This has forced the Agency to create our own unique mechanisms for maintaining compartments of information and for enforcing need-to-know and the protection of sources and methods. These control measures have typically been patched onto systems, and experience has shown that they cannot be trusted to function without some gaps or failures. 25X1

Major computer vendors such as IBM, DEC, Sperry, Data General, and Wang are developing secure operating systems that will begin to become available in FY 1985. The money requested under this initiative, therefore, will be used only to purchase, install, and evaluate these vendor-supported products. 25X1

8. Hardware/Software/Firmware Verification. The objective of the verification project is the establishment of the capability to detect the clandestine alteration of Agency information system hardware, software, and microcode for hostile purposes 25X1

Administrative, procedural, and technical measures are needed to ensure the integrity of the components and subsystems of the Agency's and Intelligence Community's (IC) information systems. Initial technical measures would employ present commercial quality-assurance tools and techniques while placing additional focus on the enhancement of these techniques and the development of new technology to meet the security and integrity objectives. 25X1

This is an ORD program due for initial funding in FY 1985. 25X1

9. Analysis and Monitoring of Advanced Technologies. This project would establish a continuing capability within the Agency to monitor, evaluate, develop, and apply advanced concepts and technology to the problems of information system security that are unique to the Agency or that require an unusually rapid turn- around. 25X1

The existence of an effective, security-focused, advanced technology monitoring and evaluation capability will permit the Agency to have a clearinghouse for advanced security-related technology. The Agency would thereby be able to anticipate, solve, or avoid dangerous information system vulnerabilities in an efficient, effective, and timely manner 25X1

Such a facility would develop, test, and evaluate new concepts for the potential impact on the security of present and future Agency information systems. 25X1

10. Tamper Detection. Information-processing equipment must be protected from compromise in order to protect the information. Suspected compromises usually call for radical response procedures such as system shutdown and full technical inspection. Present methods of intrusion detection indicate only that a room has been entered. New methods must assess whether a specific device inside the room was attacked. Reliability of the detector/indicator must be far better than in present room alarm systems to reduce the incidence of nuisance alarms 25X1

The program was started in 1984. Continuation of development efforts should lead to a tamper detection technique or family of techniques that will fit the requirements of the various computer peripheral devices. 25X1

11. Sanitization. Classified or sensitive information is stored on a variety of data storage devices, including magnetic disks. This may also apply to other devices such as display screens and semiconductor buffers whose main purpose is not long-term storage. Sanitizing is a process by which the stored information is removed from a device, usually to allow the device to undergo maintenance or otherwise to be released into a nonsecure environment. Standards and methods of sanitization have to be developed for each type of device that can store information. 25X1

Devices that can be sanitized can be released to equipment manufacturers for credit in upgrading to newer devices or for exchange when repairs are needed. Without a method of sanitization, there is too much risk of disclosing the stored information to unauthorized persons. In the latter case, the devices are usually destroyed. 25X1

This program began in FY 1983 using reprogramed funds. 25X1

Policy and Standards Initiatives

During the 18 months this working group has been meeting, we have become convinced that senior management should plug a number of gaps in the Agency's information handling policy base. Therefore, this report also recommends the creation of 5 broad, high-level policies that are essential to achieve the Agency's strategic information handling goals 25X1

1. Establish interagency information-sharing policies. Because of the immediate needs of policymakers and the rapid growth of information handling technology, many officers are demanding direct access to "everything." The traditional debate surrounding data ownership and protection between intelligence collectors and producers has intensified in the electronic age. 25X1

We cannot determine the adequacy of specific computer security programs without an agreed-upon goal. The proposed information-sharing policy is a necessary common benchmark 25X1

2. Support the development and implementation of an agency information systems minimum security standard to include telecommunications. Host systems must enforce specified minimum measures of security concerning the original data owner's decision to pass the information to a second party. Because of the link, the entire system—including its telecommunications paths—must afford resident data at least a mutually agreed-upon basic level of protection. 25X1

We should support a similar initiative for the Intelligence Community. 25X1

3. Augment the relevant Agency procurement policies to include minimum information systems security and telecommunications security standards. There are no detailed policies in place today to prohibit the purchase of information handling hardware and software that fails to enforce known security requirements. In fact, it is possible to buy devices that, depending on the threat environment and their intended use, will actually facilitate violation of these rules. 25X1

This suggested policy initiative will ensure that only information handling systems designed and engineered to permit the enforcement of applicable computer security regulations and requirements will be procured. The system configuration and the application itself will determine the extent to which these standards apply in the design, development, procurement, implementation, and operation of any automated information-processing system. 25X1

4. Consolidate the development and maintenance of an Agency capability to deliver full and timely information on hostile intelligence service threats to Agency and NFIP information systems. The collection and production of reporting about Hostile Intelligence Service (HIS) intentions and capabilities against automated information handling equipment is neither focused nor consolidated. As a consequence, our knowledge of threats and vulnerabilities from HIS is limited. In view of the potential for serious damage from a compromise, a specific unit to report against this element of intelligence would increase the confidence in the security of our systems. 25X1

5. Encourage vendor development of secure information handling and telecommunications software and hardware. Vendors have seen little public evidence of a commitment to use available electronic information safeguards on the part of the Intelligence Community. This perception actually has been the basis for decisions not to devote research dollars to security products or to develop secure hardware, software, and firmware. 25X1

Once the minimum procurement policy cited above has been agreed upon, senior Agency officials could articulate the Agency's commitment to its implementation. If the CIA, as a leader in the field, were to demonstrate an interest, this would be a positive factor in persuading vendors of the soundness of building security into their products. 25X1

Appendix A

Recommended Program Funding Level Spreadsheets

Initiative Name: System Auditing and Accountability

Executive Agent: OS/Information Systems Security Group (ISSG)
Action Office: OS/ISSG

Description of the Project. Computer security audits are being used today as the basis for detecting abnormal system activities (such as unauthorized attempts to access files) and to signal the occurrence of any unusual or potentially hostile activity. This program is still maturing—the present checks require extensive manual reviews of numerous printouts to detect problems. A program concept plan to significantly automate this auditing and accountability on all Agency systems exists, and the requested funds would implement this initiative.

Intelligence Benefit. The Agency has no real-time audit capability at present since these checks are routinely done a minimum of 24 hours after the fact. This program will develop auditing tools that will isolate and thus allow us to neutralize problems as they arise and before serious damage can result.

Status. The program began in FY 1983 using reprogramed funds. It has been included in the FY 1985 COMPUSEC initiative as an Intelligence Community effort.

Planned Use of Nonpersonal Services Funds. The initial work has been IBM mainframe specific, and additional efforts are necessary to develop a consolidated and integrated audit data base consisting of multiple systems' hardware and software activity records. Further, additional work is needed to develop tools for the relatively inexperienced security auditor who will monitor the systems afterhours and on weekends. Studies are presently under way to determine the feasibility of developing "expert systems" to analyze audit records. Early results indicate a moderate-to-good prospect of near-term success.

Utilization of Positions. There are no requested positions in FY 1985. Out-year slots will be used for system security monitors.

Resource Profile Changes. It is anticipated that the level of effort will remain high as new systems and new types of systems are brought on line, each of which will require an expansion or a retooling of the audit methodology.

Outyear Costs. Costs can be anticipated to increase circa FY 1989 as new systems come on line.

Table 1
System Auditing and Accountability

	Recommended Program Funding Level [a]							
	1985	1986	1987	1988	1989	1990	1991	1992
Total *(million dollars)*	1.0	3.3	1.5	1.5	2.5	2.5	2.5 [b]	0
Positions	0	1	1	1	1	1	1	0
High option								
Total *(million dollars)*	1.5	5.0	2.25	2.25	3.75	3.75	3.75 [b]	0
Positions	2	2	1	1	1	1	1	0
Low option								
Total *(million dollars)*	1.0	1.0	0.5	1.0	1.0	0	0	0
Positions	1	1	0	0	0	0	0	0

[a] Fiscal year.
[b] Estimated FOC.

This table is [redacted] 25X1

Initiative Name: Network Security (Summary of Subinitiatives)

Executive Agent: Office of Communications (OC)
Action Offices: OC, OS, and ODP

Description of the Project. In the next decade Agency networks will become increasingly complex and widespread in order to handle the exponential increase of information processed by the CIA. These networks will offer broader exposure and potentially greater vulnerability to security compromises by dramatically increasing the number of users with potentially unauthorized access and introducing additional vulnerabilities through the addition of network components.

Until now, network security has focused primarily on highly localized computer networks and long-haul networks. However, the merger of these networks worldwide to satisfy worldwide data-sharing requirements and to support critical Intelligence Community operations will create vastly more complex security issues that must be addressed.

In response to this need, OC must establish a formal network security program to improve network security policy, techniques, and validation tools through a mutually supportive mixture of initiatives that focus on four critical areas of networking:

- Multilevel secure operation.
- Long-haul networks.
- Gateways.
- Local area networks.

Intelligence Benefit. Provision of network security features that provide a verifiable, high level of automatic protection to information will permit the CIA and the Community to exploit the full benefits of technology. Network security is the essential ingredient that will allow the Agency to achieve its strategic information handling goal by the 1990s.

A network is more difficult to secure than a single computer system because the network's components may be dispersed and controlled by different managements. In addition, although networks evolve out of the union of communications and computers, their security issues are more than the simple union of the security issues of communications and computers. The problems in both areas combine, and new problems emerge from the interactions between multiple computers and communications lines.

This network security program will ensure that Agency networks can be used to their fullest by affording them the security required. It will examine complex technical issues as well as broad policy and standards. These policies will guide systems development, installation, and maintenance by incorporating required security features into initial system design, thus ensuring that security will be designed into systems at their inception, rather than by retrofit or patchwork. Standards will provide the criteria for evaluation of hardware and software. Another major aspect will be the establishment of a procedural framework for enforcing compliance with security requirements.

Status. This is an OC initiative due for initial funding in FY 1987. However, funds from several FY 1986/87 initiatives would be directly applicable to this Network Security Initiative:

- COMSEC capabilities, $256,000 in FY 1986.
- ADP System Audit Package, $100,000 in FY 1986; all $100,000 in FY 1987.
- Computer Security Support, all $100,000 in FY 1986.

Planned Use of Nonpersonal Services Funds. Recommended funding would be used to implement an overall network security program. The program would include development of prototype systems, development of network standards, and definition of a procedural framework for enforcement of standards and certification of Agency networks.

Utilization of Positions. The new positions will be for contract monitoring as well as providing technical support.

Resource Profile Changes. The level of effort will remain high for the first several years for program setup, then level off.

Outyear Costs.

Table 2
Network Security (Summary of Subinitiatives)

	Recommended Program Funding Level [a]						
	1985	1986	1987	1988	1989	1990	1991
Total *(million dollars)*	0.85	0.85	0.65	0.45	0.35	0.15	0.15
Positions	2	2	2	2	2	2	2

[a] Fiscal year.

This table is [ ]

25X1

Initiative Name: Network Security Subinitiative—Multilevel Operation

Executive Agent: OC
Action Offices: OC, OS, and ODP

Description of the Project. The operating mode of a network as a whole may serve as a means of protection against communications-related threats. All systems in the network, in effect, then adopt the operating mode of the network and must, therefore, meet the minimum security requirements of that mode. In a multilevel mode, the system concurrently stores and processes data of different security levels, allows concurrent access to data by users having different security clearances and need-to-know, and automatically maintains proper separation between the levels. The system may be open for uncleared as well as cleared users, or, if the environment is too threatening, it may be closed with no uncleared users.

CIA networks presently operate in a system-high environment such that anyone with direct, unescorted access is cleared to staff standards. However, as the demand increases for Agency networks to interconnect with Intelligence Community systems, they must be capable of operating in a multilevel-secure mode to allow concurrent access by users having different security clearances and need-to-know, while maintaining the proper separation between the levels. Even within the Agency, a computer operating system-high mode may need to connect to a multilevel-secure computer, forming a network.

Intelligence Benefit. National policymakers require data delivered from a variety of network sources, including BIOSTAR, ALLSTAR, SAFE, CAMS, COINS, and DESIST. Network interoperability can provide this capability. Also, networks such as CIA-MERCURY, Intelligence Community–COINS, and Defense Communications Agency–DDN terminate in the same overseas locations or intersect at major nodal points. In order to permit maximum flexibility for traffic handling in a crisis situation, these networks should be capable of interoperating in contingency situations. Multilevel secret networks can support this national objective of interoperablity by allowing separately managed packet-switched systems to intercommunicate securely via gateways, protocol standardization, routing tables, and so forth.

Table 3
Network Security Subinitiative—
Multilevel Operation

	Recommended Program Funding Level [a]						
	1985	1986	1987	1988	1989	1990	1991
Total *(million dollars)*	0.3	0.3	0.2	0.2	0.1	0	0
Positions	0	0	0	0	0	0	0

[a] Fiscal year.

This table is [redacted] 25X1

CIA computers operating at different security levels must also be able to interoperate; multilevel-secure network techniques would permit this.

Status. This program has been included in the overall OC Network Security Initiative due for initial funding in FY 1987.

Planned Use of Nonpersonal Services Funds. This funding is for the purpose of study of multilevel security issues and the development of a prototype network architecture that would support Agency requirements for multilevel secure information handling. The effort would address the operation of local-area and wide-area nets as a whole, as well as individual network components such as gateways, communications processors, and multiplexors.

Gateways are particularly important from an internetwork standpoint. Internetwork security requires gateways designed with security features from the beginning. These features must allow secure multilevel internetwork communication between two networks. This funding would support the development of a prototype gateway architecture that would support almost all Agency internetwork connections.

Multilevel-secure communications processors, which in some cases could serve as gateways, must also be investigated.

Utilization of Positions. This program requires no increase in positions.

Resource Profile Changes. The level of effort will peak in FY 1985 and FY 1986, then decline over the next three years.

Outyear Costs. The outyear costs will support implementation of prototype systems in target networks.

Initiative Name: Network Security Subinitiative—Standards Development

Executive Agent: OC
Action Offices: OC, OS, and ODP

Description of the Project. The Agency has placed its principal security dependency on an extensive system of physical and personnel security augmented by several standard measures for computer systems such as a password system for terminals. To keep pace with the evolution of networks, however, a clear, firm, and enforceable policy and standard baseline is essential. Because it appears that the Director of Central Intelligence Directive No. 1/16 (DCID 1/16) for Security of ADP Systems and Networks will be revised to include top-level policy for telecommunications networks, this revised policy will form a basis for a new body of lower-level standards that OC must define. Although many of these lower-level standards will be developed by the DOD Computer Security Center, OC must adapt them for Agency use as well as define new ones for the unique Agency networks. The objective of this project is to define such baseline standards for:

- Local-area networks (LANs).
- Long-haul networks.
- Gateways.

Intelligence Benefit. Security cannot be retrofitted into a network system. A comprehensive set of network security policies and standards will guide systems development and maintenance by incorporating required security features into the initial systems design. It will also provide the security criteria to be applied in evaluating whether the network provides adequate protection.

Status. This program has been included in the OC Network Security Initiative due for initial funding in FY 1987.

Planned Use of Nonpersonal Services Funds. This funding provides for contractor assistance in defining telecommunications standards, a procedural framework for managing security, and for running a quality assurance activity designed to enforce standards and procedures. The standards will be used for evaluating network security and should reflect National Policy and Directives as well as OC/COMSEC technical standards. Standards should apply to both hardware/software products as well as network implementations.

Utilization of Positions. One staff position is required to assist contractors and then run the quality-assurance activity.

Resource Profile Changes. The level of effort will remain high over the first three years in order to define the standards and establish initial procedures, then it will level off.

Outyear Costs. The outyear costs will provide for follow-on quality-assurance activity to ensure standards and procedures are followed and that systems provide adequate protection.

Table 4
Network Security Subinitiative—
Standards Development

	Recommended Program Funding Level [a]						
	1985	1986	1987	1988	1989	1990	1991
Total *(million dollars)*	0.25	0.25	0.25	0.05	0.05	0.05	0.05
Positions	1	1	1	1	1	1	1

[a] Fiscal year.

This table is [redacted] 25X1

Initiative Name: Network Security Subinitiative—Audit Package

Executive Agent: OC
Action Offices: OC and OS/ISSG

Description of the Project. Network security audits, like computer audits, report on unusual or potentially hostile network activities, such as unauthorized attempts to establish network connections. To the extent that these audit trails are independently handled by a network host, network audits will resemble individual computer auditing. However, in an automated network, audit information will be accumulated and then sent to one or more of the network elements that have been assigned responsibility for security. This introduces an additional vulnerability to the audit records themselves.

The purpose of this project is to develop a secure automated audit package to be used in the certification of networks.

Intelligence Benefit. Intelligence without security is not intelligence. Auditing is the primary means of certifying that intelligence information is being handled securely within a network, in accordance with established standards.

As stated in the Director of Central Intelligence Directive No. 1/16 (DCID 1/16) for ADP and Network Security, all ADP systems must be recertified annually. As a result of the OC Recapitalization Program, a new series of automated switches, network access systems, and a variety of automated terminal systems will be introduced in the near future. On the basis of the total numbers of ADP systems to be recertified and the shortage of personnel available, there is a current shortfall in the ability to comply with the DCID 1/16 recertification requirement. The audit package to be developed would comply with DCID 1/16 requirements, be operable by COMSEC officers who are not skilled technicians, and reduce system downtime for testing.

Table 5
Network Security Subinitiative—
Audit Package

	Recommended Program Funding Level [a]						
	1985	1986	1987	1988	1989	1990	1991
Total *(million dollars)*	0.2	0.2	0.1	0.1	0.1	0	0
Positions	0	0	0	0	0	0	0

[a] Fiscal year.

This table is Confidential.

Status. This program has been included in the overall OC Network Security Initiative due for initial funding in FY 1987. However, the entire OC FY 1986/87 initiative for the ADP System Audit Package would be applicable to this portion of the program.

Planned Use of Nonpersonal Services Funds. The FY 1985 funding is for one person-year of study and development of a portable system to interrogate host system software to meet recertification requirements. The FY 1986 funding is for the development of a prototype system and to initiate a follow-on for production systems. Outyear funds will be used for implementation in new and existing systems.

Utilization of Positions. This program requires no increase in positions.

Resource Profile Changes. The level of effort will remain high for two years to allow for development of a prototype system, then decline for implementation in new and existing systems.

Outyear Costs.

Initiative Name: Network Security Subinitiative—Evaluation and Certification

Executive Agent: OC
Action Office: OC

Description of the Project. Once countermeasures have been implemented, their effectiveness must be formally certified based on defined standards. This new initiative is required to allow for conducting technical evaluations and formal certification of network products, including communications processors, multiplexors, and gateways; as well as entire network systems, to determine conformance to OC Network Security standards. The program will support technical evaluation by participating in the procurement and implementation of new networks. Such participation involves identifying security requirements for inclusion in Requests for Proposal and assisting in evaluation of the contractor responses.

The program will also establish a formal certification program for networks, based on an evaluation of the effectiveness of security countermeasures.

Table 6
Network Security Subinitiative—
Evaluation and Certification

	Recommended Program Funding Level [a]						
	1985	1986	1987	1988	1989	1990	1991
Total *(million dollars)*	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Positions	1	1	1	1	1	1	1

[a] Fiscal year.

This table is [redacted] 25X1

Intelligence Benefit. Network interoperability requires assured security. A network evaluation and certification will eliminate the uncertainty surrounding the security of Agency information networks as these networks become more complex and interconnected with Intelligence Community networks.

Status. This program has been included in the overall OC Network Security Initiative due for initial funding in FY 1987. The current MERCURY Security Analysis Initiative would be applicable to this program.

Planned Use of Nonpersonal Services Funds. The new funding will be used to provide supplemented expertise in both network security evaluation and certification. It includes the on-going security analysis initiative for the Agency's major long-haul network, MERCURY, and will be expanded to address a new series of automated switches, network access systems, and a variety of automated terminal systems resulting from the OC Recapitalization Program. It will also address local-area networks (LANs) and gateways.

Utilization of Positions. The new staff position would act as a COTR as well as a focal point for all network evaluation and certification activities. Staff positions would also participate in technical evaluation and security certification by participating in the procurement and implementation.

Resource Profile Changes. It is anticipated that the level of effort will remain high as new network systems are brought on line, each of which will require evaluation and certification.

Outyear Costs. Outyear costs will be comparable to initial costs.

Initiative Name:
Stronger Access and Authentication Controls

Executive Agent: OS/ISSG
Action Office: OS/ISSG

Description of the Project. Agency users of automated information handling systems gain access today by simply matching their unclassified userid with a classified password. Although the secrecy of this password provides a measure of access control, experience shows that this method is far from fail-safe. Indeed, there have already been a number of security incidents directly attributable to password abuse.

With a rapidly expanding user community and extensive all-source access requirements, the strengthening of access controls is becoming increasingly important. In the search for a more positive authentication of users at the terminal, there must be a greater emphasis on "layered passthrough," particularly for users located away from Headquarters.

As the Agency moves toward automation, many of the administrative and management controls of our paper offices will be replaced with their electronic equivalents but without the human controls that allow these systems to operate today. The release of cables and the signing of vouchers are but two examples of areas where more positive identification and authentication at the terminal will be required.

Intelligence Benefit. As access to our own and other data bases across local- and long-haul networks becomes more commonplace, it will become even more important to enforce a trusted system of positive identification and authentication. This program will supplement today's access systems as a program of common concern for the entire Intelligence Community.

Status. The program began in FY 1983 using reprogramed funds. It has been included in the FY 1985 COMPUSEC initiative as an Intelligence Community effort.

Planned Use of Nonpersonal Services Funds. There are a number of promising hardware- and software-based approaches to enforcing stronger access controls available today. IBM, for example, has a signature verification device currently undergoing testing within ISSG and IMS. The funds would be used to evaluate a number of promising approaches and to then actually utilize the equipment wherever increased controls are warranted.

Utilization of Positions. This program requires no increase in positions.

Resource Profile Changes. None.

Outyear Costs. Costs can be anticipated to increase circa FY 1989 as new systems come on line.

Table 7
Stronger Access and Authentication Controls

	Recommended Program Funding Level [a]						
	1985	1986	1987	1988	1989	1990	1991
Total *(million dollars)*	0.5	0.5	0.25	0.25	0.25	0.5	0.5
Positions	0	0	0	0	0	0	0
High option							
Total *(million dollars)*	1.0	1.0	1.0	0.5	0.5	1.0	1.0
Positions	0	0	0	0	0	0	0
Low option							
Total *(million dollars)*	0.25	0.25	0.10	0.10	0.10	0	0
Positions	0	0	0	0	0	0	0

[a] Fiscal year.

This table is [ ]

25X1

Initiative Name: Advanced Encryption Techniques Subinitiative—File and Data Base Encryption Development

Executive Agent: OC
Action Office: OC, OS/ISSG, and ODP

Description of the Project. File encryption offers protection against attacks on an inadvertent disclosure of data stored on magnetic disk and tape. This program would allow for the analysis, design, and development of prototype file encryption devices to be used by several OC components: DDA/ODP, for general use; DDO/IMS, for the Craft system; and DI for use in the analysts' personal computers.

File encryption applied to ODP data bases and other software will allow more secure general usage, including archiving, while reducing physical security requirements. Craft file encryption will eliminate paper file holdings in the station that allows an increase in data holdings by the station. It will also obviate much of the emergency destruction problem in the foreign field. DI file encryption will provide individual protection for the analysts' personal computers and associated floppy disks.

Intelligence Benefit. Storage media are becoming increasingly smaller, although their capacity to hold information is becoming increasingly larger. Consequently, they are an evermore attractive target for hostile attack. They also present greater challenges to enforcing data compartmentation and restricting need-to-know access. File encryption provides assurance against security threats such as intrusion, theft, and spillage, while at the same time providing a means to enforce access controls based on data compartmentation and need-to-know.

Table 8
Advanced Encryption Techniques Subinitiative—File and Data Base Encryption Development

	Recommended Program Funding Level [a]						
	1985	1986	1987	1988	1989	1990	1991
Total *(million dollars)*	0.25	0.25	0.25	0.15	0.15	0	0
Positions	0	0	0	0	0	0	0

[a] Fiscal year.

This table is [redacted] 25X1

Status. This program is a COMSEC new initiative for FY 1985 that was submitted, but not approved.

Planned Use of Nonpersonal Services Funds. FY 1985 funding will be used to evaluate the feasibility of techniques and to select recommended design approaches. FY 1986 funding will be used to design and produce prototype devices for the Craft Wang terminals, ODP data bases, and DI personal computers. FY 1987-89 funding will allow follow-on procurement of first Craft production models and prototype devices for ODP and DI applications. Outyear procurement of file encryption devices will be funded by user offices.

Utilization of Positions. This program requires no increase in positions.

Resource Profile Changes. None.

Outyear Costs. Outyear costs will allow for design and implementation of techniques in other applications.

Initiative Name: Advanced Encryption Techniques Subinitiative—End-to-End Encryption Development

Executive Agent: OC
Action Office: OC
Description of the Project. As the increasing demand for more user data terminals and the use of electronic data grows, new security measures must be implemented to provide data compartmentation and to protect the need-to-know principle. There is a current shortfall in the ability to protect data in the growing local-area networks (LANs) and overseas deployment is either not feasible or is prohibitively costly. The development of both hardware and software end-to-end data encryption techniques will both provide greater data security and reduce procurement, installation, and maintenance costs.

Table 9
Advanced Encryption Techniques
Subinitiative—End-to-End
Encryption Development

	Recommended Program Funding Level [a]						
	1985	1986	1987	1988	1989	1990	1991
Total *(million dollars)*	0.25	0.15	0.1	0	0	0	0
Positions	0	0	0	0	0	0	0

[a] Fiscal year.

This table is [ ]

25X1

End-to-end encryption provides a continuous encrypted data path from source user to destination user. This approach minimizes the risk of spillage, interception, and unauthorized access, while improving the authenticity of the message at the destination. This program would focus on developing a modern end-to-end encryption system that would include an automated key distribution system to electronically distribute matching keys from a control center to the widely separated pairs of crypto devices.

Intelligence Benefit.

Status. This program is an OC COMSEC initiative due for initial funding in FY 1986.

Planned Use of Nonpersonal Services Funds. FY 1985 funding will allow procurement of prototype hardware equipment and an effort toward a software implementation. The FY 1986 funding will result in the implementation of translator software for installation of the approved encryption algorithm in a large number of Agency data terminal types. Outyear funding will support additional studies and implementations.

Utilization of Positions. This program requires no increase in positions.

Resource Profile Changes. None.

Outyear Costs. Outyear funding will be used for additional studies and implementation.

Initiative Name: Control of Data Storage Media

Executive Agent: OS
Action Offices: OS/ISSG, ORD, and OS/Technical Security Division (TSD)

Description of the Project. Data must be protected from unauthorized or accidental disclosure while it resides on various storage media such as magnetic tape, rigid disk, and flexible disk. Control methods used elsewhere, such as tagging transportable media, will be explored to detect attempts to remove the media from authorized areas. New technical labeling methods will also be investigated to prevent the accidental mishandling of media. The project will not be limited to magnetic media. As new technologies of data storage media come into use, they will be included.

Intelligence Benefit. At present, there is no reliable method of detecting attempts to remove data storage media from a facility, yet many devices are capable of concealment on a person's body. This project could provide a technical means of detecting certain types of commonly used storage media as persons pass a control point.

Status. Previous efforts in this area have not yet produced a solution to the problem. A new look, which is closely linked to physical and procedural security measures, is recommended.

Planned Use of Nonpersonal Services Funds. The indicated funding would first be used for research into promising solutions. In FY 1987 it is planned that the proposed solution(s) would be implemented in a hardware system that can be used at points of exit from a facility.

Utilization of Positions. During the initial phase, the work will be performed by contractors. No new government positions will be needed as long as there are already sufficient personnel to monitor the contractors' work. During the implementation phase, it is expected that one or more new positions will be needed.

Resource Profile Changes. Primary research will be done in FY 1985 and FY 1986. A peak in the costs is expected during the implementation or development and engineering phase from FY 1987 to FY 1989. This period overlaps with the installation and maintenance phase that continues at least through FY 1990.

Outyear Costs. This is a high-risk research and development effort. Outyear activities depend on successful conclusion of the phase-one design effort. If no solutions are identified during the initial work, no costs or personnel will be needed beyond that point.

Table 10
Control of Data Storage Media

	Recommended Program Funding Level [a]							
	1985	1986	1987	1988	1989	1990	1991	1992
Total *(million dollars)*	0.2	0.3	0.4	0.4	0.3	0.1	0	0
Positions	0	0	1	1	1	1	0	0
High option								
Total *(million dollars)*	0.2	0.3	0.5	0.5	0.4	0.2	0.1	0
Positions	0	1	2	2	2	1	1	0
Low option								
Total *(million dollars)*	0.2	0.3	0.3	0.3	0.2	0.1	0	0
Positions	0	0	1	1	1	1	0	0

[a] Fiscal year.

This table is [ ]

25X1

Initiative Name:
Automated Labeling

Executive Agent: OS/ISSG
Action Offices: OS/ISSG, ODP, and ORD

Description of the Project. Automated labeling is a means of enforcing a deliberate management decision as to which mandatory and discretionary controls are required for a specific element of information in a data base. The computer is used as the primary means of enforcing this process by comparing the data's sensitivity controls (that is, classification caveats and discretionary labels such as "Exclusive For" and "Orcon") with the potential recipients' access authorizations.

Intelligence Benefit. At present, there is no way to match the classification of a data element to a potential recipient's clearances and access authorizations (including compartmentation and need-to-know) on more than a very limited scale. Because of this significant amounts of information are either not shared as widely as is desirable, or are shared and thereby subjected to the risk of unauthorized disclosure.

Table 11
Automated Labeling

	Recommended Program Funding Level [a]							
	1985	1986	1987	1988	1989 [b]	1990	1991	1992
Total *(million dollars)*	1.4	3.2	2.094	1.937	2.7	3	3.0 [c]	3.0 [c]
Positions	2	1	1	1	1	1	1 [c]	1 [c]
High option								
Total *(million dollars)*	1.4	3.2	2.6	2.4	3.2	3.5	3.5	3.5
Positions	2	2	2	2	2	2	0	0
Low option								
Total *(million dollars)*	0.9	2	1	1	1	0.5	0.5	0
Positions	2	1	0	0	0	0	0	0

[a] Fiscal year.
[b] Estimated IOC.
[c] Unbudgeted.

This table is [redacted] 25X1

Status. A COMPUSEC initiative due for initial funding in FY 1985.

Planned Use of Nonpersonal Services Funds. Automated labeling (during FY 1985) is a two-phase effort to study and implement a trusted system for machine readable data. The initial phases will involve defining the problem, then choosing the most promising path leading toward a solution. Responsibility for coordinating and monitoring the in-house and contractors' efforts will rest with the Information Systems Security Group of the Office of Security.

Utilization of Positions. Because of the unique expertise required, it is planned to have a Project Officer and a Technical Adviser assigned to a (newly created) ISSG Special Projects Office to act as the focal points for all COMPUSEC program-related work.

Resource Profile Changes. It is anticipated that the level of effort will peak in FY 1986 due to the one-time costs and then level off.

Outyear Costs. This is a high-risk research and development effort whose dimensions will not be fully understood until the phase-one problem definition is completed. Outyear costs should be viewed accordingly.

Initiative Name: Secure Multilevel Processing Operating Systems Applications Software Multilevel Data Bases

Executive Agent: OS/ISSG
Action Offices: OS/ISSG and ODP

Description of the Project. The inability to enforce data separation by classification level and compartments as well as according to control restrictions such as Orcon and Exclusive For is a major shortfall in today's intelligence processing environment.

The CIA's computer centers operate in a pseudosystem high environment. Although everyone with direct, unescorted access to the facilities and their information is cleared to staff standards, not everyone has been granted need-to-know approval for all of the resident data. This has caused the Agency to "home brew" unique mechanisms for maintaining two or more compartments of information and for enforcing need-to-know and the protection of sources and methods. These control measures have typically been patched onto systems, and experience has shown that they cannot be trusted to function without some gaps or failures.

Intelligence Benefit. The use of true multilevel operating systems, applications software, and data bases will allow us far more flexibility in the design and implementation of information handling systems and networks.

Status. Major computer vendors such as IBM, DEC, Sperry, Data General, and Wang are developing B2 or higher secure operating systems that will begin to become available in FY 1985.

Planned Use of Nonpersonal Services Funds. The requested funds would be used to establish demonstration systems so that we can gain practical, on-site experience and make pragmatic judgments regarding the vendors' new software releases. Furthermore, test bed use of these systems would signal our commitment to the concept of information systems security. No monies will be spent on actual software development.

Utilization of Positions. There are no positions required to implement this initiative.

Resource Profile Changes. None.

Outyear Costs.

Table 12
Secure Multilevel Processing

	Recommended Program Funding Level [a]							
	1985	1986	1987	1988	1989	1990	1991	1992
Total (*million dollars*)	0.2	0.2	0.2	0.1	0.1	0.1	0.1	0.1
Positions	0	0	0	0	0	0	0	0

[a] Fiscal year.

This table is [ ]

25X1

Initiative Name: Hardware/Software/ Firmware Verification

Executive Agent: ORD
Action Office: ORD and ISSG

Description of the Project. The objective of the verification project is the establishment of the capability to detect the clandestine alteration of Agency information system hardware, software, and microcode for hostile purposes.

Intelligence Benefit. Administrative, procedural, and technical measures are needed to ensure the integrity of the components and subsystems of the Agency's and Intelligence Community's information systems. Initial technical measures would employ present commercial quality assurance tools and techniques while placing additional focus on the enhancement of these techniques and the development of new technology to meet the security and integrity objectives.

Status. This is an ORD program due for initial funding in FY 1985.

Planned Use of Nonpersonal Services Funds. Requested funding will be used to address requirements defined by the FY 1985 initial study.

Utilization of Positions. Because of the expertise required, the project officer/ technical adviser should act as a focal point for related activities.

Resource Profile Changes. Both posistions and funding will increase after FY 1986.

Outyear Costs. The cost will depend on the technical, procedural, and administrative issues and requirements identified during the initial study phase.

Table 13
Hardware/Software/Firmware Verification

	Recommended Program Funding Level [a]						
	1985	1986	1987	1988	1989	1990	1991
Total (*million dollars*)	0.3	1.5	0.5	0.5	0.3	0.1	0.3
Positions	1	1	3	3	3	3	3
High option							
Total (*million dollars*)	0.5	2	0.7	0.5	0.5	0.5	0.5
Positions	2	2	5	5	5	5	5
Low option							
Total (*million dollars*)	0.2	1	0.4	0.4	0.2	0.2	0.2
Positions	1	1	2	2	2	2	2

[a] Fiscal year.

This table is [redacted] 25X1

Initiative Name: Analysis and Monitoring of Advanced Technologies

Executive Agent: ORD
Action Office: ORD

Description of the Project. This project would establish a continuing capability within the Agency to monitor, evaluate, develop, and apply advanced concepts and technology to the problems of information system security that are unique to the Agency or that require an unusually rapid turnaround.

Intelligence Benefit. The existence of an effective, security focused, advanced technology monitoring and evaluation capability will permit the Agency to have a clearinghouse for advanced security-related technology. The Agency would thereby be able to anticipate, solve, or avoid dangerous information system vulnerabilities in an efficient, effective, and timely manner.

Status. This is an ORD program due for initial funding in FY 1986.

Table 14
Analysis and Monitoring of Advanced Technologies

	Recommended Program Funding Level [a]						
	1985	1986	1987	1988	1989	1990	1991
Total *(million dollars)*	0.5	2	2	2.5	2.5	3.0	3.0
Positions	3	5	6	6	6	6	6
High option							
Total *(million dollars)*	1.0	2.5	3.0	3.0	4.0	4.0	4.0
Positions	5	7	8	8	8	8	8
Low option							
Total *(million dollars)*	0.3	1.0	1.0	1.0	2.0	2.0	2.0
Positions	2	3	4	4	4	4	4

[a] Fiscal year.

This table is [ ]

25X1

Planned Use of Nonpersonal Services Funds. Requested funding will be used to establish initial facilities and support structures, plus initiation of the first research/evaluation to be undertaken by this effort.

Utilization of Positions. At least three positions including adminstrative, technical, and support personnel are initially projected.

Resource Profile Changes. Positions and funding will increase during the establishment of the analysis and monitoring capability. Positions and funding will level off as the capability enters its ongoing phase.

Outyear Costs. The costs will depend on technical and procedural issues identified by the analysis.

Initiative Name: Tamper Detection for Computer Peripheral Devices

Executive Agent: OS/ISSG
Action Office: OS/ISSG, IMS, and OC
Description of the Project. Computer peripheral devices are becoming so widespread in the Agency environments domestically and abroad that conventional alarm systems cannot be used to protect all of them at the desirable level of security. Attempts to compromise data terminals, printers, and other information processing equipment and their signal lines will have to be studied. Alternative methods of detecting and reporting tamper attempts will have to be developed.

Table 15
Tamper Detection for Computer Peripheral Devices

	Recommended Program Funding Level [a]							
	1985	1986	1987	1988	1989	1990	1991	1992
Total *(million dollars)*	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0
Positions	0	0	0	0	0	0	0	0
High option								
Total *(million dollars)*	0.4	0.5	0.4	0.4	0.4	0.4	0.4	0
Positions	1	1	1	1	1	1	1	0
Low option								
Total *(million dollars)*	0.15	0.15	0.15	0.15	0.15	0.15	0.15	0
Positions	0	0	0	0	0	0	0	0

[a] Fiscal year.

This table is [redacted] 25X1

Intelligence Benefit. Intelligence information processing equipment must be protected from compromise in order to protect the information. Suspected compromises usually call for radical response procedures such as system shutdown and full technical inspection. Present methods of intrusion detection indicate only that a room has been entered. New methods must assess whether a specific device inside the room was attacked. Reliability of the detector/indicator must be far better than in present room alarm systems to reduce the incidence of nuisance alarms.

Status. The program was started in 1984. Continuation of development efforts should lead to a tamper detection technique or family of techniques that will fit the requirements of the various computer peripheral devices.

Planned Use of Nonpersonal Services Funds. Beginning in FY 1985 funds will be used for producing prototype detectors for evaluation. The manufacture of production lots of an accepted device will follow in late FY 1985 or in FY 1986. Further development is expected from FY 1986 through the outyears for methods to detect tamper attempts on the signal lines.

Utilization of Positions. This program requires no new positions in the recommended program funding.

Resource Profile Changes. None.

Outyear Costs.

Initiative Name: Sanitization

Executive Agent: OS/ISSG
Action Office: OS/ISSG, OS/TSD, and ORD

Description of the Project. Classified or sensitive information is stored on a variety of data storage devices, including magnetic disks. This may also apply to other devices such as display screens and semiconductor buffers whose main purpose is not long-term storage. Sanitizing is a process by which the stored information is removed from a device, usually to allow the device to undergo maintenance or otherwise to be released into a nonsecure environment. Standards and methods of sanitization have to be developed for each type of device that can store information.

Intelligence Benefit. Devices that can be sanitized can be released to equipment manufacturers for credit in upgrading to newer devices or for exchange when repairs are needed. Without a method of sanitization, there is too much risk of disclosing the stored information to unauthorized persons. In the latter case, the devices are usually destroyed.

Status. This program began in FY 1983 using reprogramed funds.

Planned Use of Nonpersonal Services Funds. The initial work in sanitization has been in magnetic disk erasure studies. This phase of the project will continue at least through the end of FY 1985. As new storage devices or technologies emerge, a continuing program to develop sanitization methods will be needed.

Utilization of Positions. No new position is requested for FY 1985. One technical employee will spend approximately half of his time on this project.

Resource Profile Changes. It is anticipated that the level of effort will remain high as new products and new storage technologies are introduced.

Outyear Costs. Costs can be expected to remain fairly steady except for a gradual trend upward caused by economic inflation.

This appendix is Confidential.

Table 16
Sanitization

	Recommended Program Funding Level [a]							
	1985	1986	1987	1988	1989	1990	1991	1992
Total *(million dollars)*	0.15	0.15	0.15	0.18	0.18	0.18	0.18	0
High option								
Total *(million dollars)*	0.3	0.3	0.3	0.3	0.4	0.4	0.4	0
Low option								
Total *(million dollars)*	0.1	0.1	0.1	0.1	0.2	0.2	0.2	0

[a] Fiscal year.

This table is [ ]

25X1

Appendix B

A View of Information Handling in 1992

Paced by the continuing microprocessor evolution, the growing use of telecommunications networks, and the increasing sophistication and usefulness of packaged software, the Age of Information has fundamentally changed the manner in which the Agency operates. Two facts underscore the computer's role in the larger context of our future society: personal computers are being accepted by society at a faster rate than was the telephone, and an IBM-PC alone is produced every seven seconds. The explosion of technology within the Agency means that the vulnerabilities of our information handling systems are actually increasing. The following represents one possible scenario for the 1992 processing environment from the user's viewpoint. 25X1

Nearly all employees located both domestically and overseas will use a workstation that provides sophisticated word processing, electronic mail, access to cable traffic, and other forms of communication such as video and audio. 25X1

These workstations are evolving from three dominant trends in information processing: the rapid introduction of and advancement in microcomputer technology; the development of complex, but user-friendly packaged software tools for personal computers; and the constant growth of information-sharing and networking capabilities. 25X1

Despite the current emphasis on microcomputers, mainframes will be used extensively as switching devices and for providing access to massive information archives for downloading information to the workstation. Mainframes will still be used for huge computationally intensive applications such as scientific modeling work. 25X1

Wherever the possibilities offered by both centralized and distributed processing take us, there will always be a need for centralized services of common concern. Information systems security will be one of them 25X1

The machine-human interface will be highly refined, requiring less computer literacy to manipulate information. Most employees will profitably use word processing, graphics, data base management systems, and spreadsheet capabilities provided by the workstation. Specialized commercially developed software of many different types will be available for specific functions. 25X1

There will also be marked changes in the interaction among our people. Highly developed communications networks will allow extensive and immediate interconnection of Agency employees throughout the world. These network facilities will also be characterized by high speeds, huge volume throughput, and the ability to handle all electrical forms of information through the same transmission devices. These include voice, image, character, other digital, and possibly analog information. 25X1

The volume of information stored on Agency computers by 1992 will increase by several orders of magnitude. New collection systems, the storage of large masses of historical data, and a broadening range of topics upon which information is collected will each cause significant increases. Office automation, increased communications storage requirements, and storage of data in the form of graphs, charts, and spreadsheets will also drive this trend. 25X1

Foreign and domestic unclassified data bases will provide a new wealth of information that we must be able to access and download securely by the same workstations used for processing classified information. 25X1

Advances in hardware and software technology will accommodate the increasing need for efficient information storage, but maintaining the reference capabilities needed for retrieval of desired information will become a problem. 25X1

The workstations of 1992 will have high-resolution, color graphics capabilities. Lap-top microcomputers will accelerate the trend toward highly portable, personalized computing. The merging of text and graphics will be routine and the production of the graphics will become more the responsibility of the person writing the text. One form of graphics display we may see by 1992 is the three-dimensional laser hologram. 25X1

Much of what we now recognize as interactive, or online computing, will be transformed into processing at the workstation in 1992. Response time will be a function solely of what the individual user is doing at his workstation. Batch processing, as we now know it, will continue to be used for routine, repetitive tasks. For example, analysts covering a specific area or topic will use unattended, time-triggered routines to get updates on a daily or weekly basis. 25X1

Software development will be more like an engineering task, dominated by system integration work. Applications programing, as we now know it, will be more of an art form to be used for special, complex applications that defy the integration of existing software tools. 25X1

In another area of software development, advanced information handling concepts will be used extensively to glean desired information out of the masses of information that will be flowing into the Agency and to augment the analysis process by going through some of the same processing steps that would be performed by a seasoned analyst. 25X1

There may be a continuous, automated examination of requirements based on current knowledge of different topics. Advanced information processing concepts will be used to complement this function. These systems could also automatically trigger requirements based on outside factors such as wire service reports or analysis of broadcasts. 25X1

Optical character recognition facilities will convert books, magazines, and other printed matter into machine-readable form. Similarly, voice recognition technology will convert audio broadcasts into machine-readable form. In many cases, however, that capability will not be needed; many foreign voice and video broadcasts will be captured in their original format for later playback at the workstation. Facsimile transmission systems will operate with high resolution and color, and at very rapid transmission rates. 25X1

The entire intelligence production and packaging system will be automated, with information transmitted electronically (or electro-optically) from analyst to reviewers, and back to the analyst for changes. The coordination process will similarly be conducted through electronic means to some extent. After review and coordination are completed the "document," still in electronic form, will go through an automated publishing network. Finally, dissemination will be in two forms: printed for some customers; electronic for others. 25X1

We can also anticipate that products on a broader range of topics will be securely disseminated to a wider range of customers by 1992, particularly if the Agency becomes more involved in tactical support to military and diplomatic personnel. 25X1

Appendix C

Threats, Risks, and Vulnerabilities

The CIA's longstanding approach to information control is unique in the government, reflecting our requirement that compartmentation, need-to-know, and the protection of sources and methods requires strict control of the total number of persons with access to information. This view holds that a vulnerability can be identified whether or not an actual threat to exploit that vulnerability exists, and that the reduction of vulnerabilities is a goal in and of itself. 25X1

We now depend heavily on procedural and personnel security as well as physical isolation to protect our electronic information handling systems. Our belief that in 10 years these measures will no longer be an adequate shield is the major conclusion reached by the working group during its review of threats, risks, and vulnerabilities 25X1

This section has not attempted to address the multitude of details that arise in the operation of a typical resource-sharing, networked computer system. Instead, it provides a brief overview of the complex nature of the problem. Although the specific flaws touched upon above can be collected under the five major headings of physical surroundings, hardware, software, communications links, and personnel security and procedures, the overall safeguarding of information is achieved by a combination of protection features working together to seal off these potential vulnerabilities 25X1

Computer crimes are being reported with increasing frequency. It comes as no great surprise that the very nature of modern computers and their communications links has created serious security vulnerabilities. Simply stated, modern information systems are ill equipped to prevent the unauthorized disclosure of information, the unsanctioned modification of data, and the sudden denial of critical services. Today's computing equipment was designed to facilitate data flow rather than restrict it; however, the owners, processors, and users of Agency data routinely expect computers to perform security functions for which they were never designed. Compounding these problems, system designers and security specialists lack many of the hardware and software utilities they require—the tools simply do not yet exist. 25X1

Computers can store far more information than any single safe. The new forms of storage media can compact tremendous amounts of data into small and easily transportable forms that are both hard to inspect and detect. The common 3.5-inch floppy diskette, for example, can now store almost a million bytes of data—almost 500 typed pages. 25X1

Computers are often interconnected and access to one can mean entry to many. They are remotely accessible, allowing unauthorized entry at low personal risk. Modern information handling systems are also programmable, sometimes causing them to become active participants in surrendering their data. They are now so complex that they can unknowingly contain inadvertent problems or induced flaws (for example, trapdoors and trojan horses), which can allow unauthorized access. [redacted] 25X1

Networks emerge when computer systems interconnect via communications lines, requiring a set of protocols that specify how the systems can communicate. In the next decade, CIA networks will become increasingly complex and widespread in order to handle the tremendous growth in CIA data-sharing requirements worldwide and to support the increasing dependency of critical Intelligence Community operations. [redacted] 25X1

These networks will offer broader exposure to security threats by dramatically increasing the potential for unauthorized access. Such networks will also create complex multilevel security issues when computers, indeed networks, operating at one security level have to interoperate with computers operating at a different level. [redacted] 25X1

Other security issues common to ADP systems, such as access controls, identification, authentication, and auditing present far more complex challenges for networks than for single computer systems [redacted] 25X1

The availability of powerful and convenient lap-top and hand-held devices will further bypass our present access, authentication, and control procedures. Dial-up capabilities are gaining widespread acceptance in the industry and have become the source of the most publicized computer problems. [redacted] 25X1

Computers are extremely efficient, deliberately providing useful tools for the extraction of data. They are their own recordkeepers, so traces of illegal entry can be erased. Finally, computers have already become indispensable, so that repairs are often made on systems while they are in operation. [redacted] 25X1

Because the majority of vendor-supplied hardware and software is inadequate for our security requirements, CIA computer centers operate in an environment in which strict compartmentation and need-to-know is impossible to guarantee. This has forced the Agency to create our own unique mechanisms for maintaining compartments of information and for enforcing need-to-know and the protection of sources and methods. These control measures have typically been patched onto systems, and experience has shown that they cannot be trusted to function without some gaps or failures [redacted] 25X1

Access controls, user identification and authentication, audit trails, and individual accountability mechanisms strong enough to meet our requirements are not yet embedded in the systems the Agency has chosen for data processing. There are also human vulnerabilities associated with the average system. Acts by individuals can accidentally or deliberately jeopardize system security [redacted] 25X1

In dealing with system security vulnerabilities, it is clear that the various potential problems cannot be viewed individually. Almost any attempt to subvert a system will necessarily involve both deliberate acts intended to create or exploit weaknesses and someone in a position to take action. Thus, espionage is often based on a combination of deficiencies and access. A minor (and perhaps acceptable) weakness in one area, in combination with shortcomings in seemingly unrelated activities, may add up to a serious potential for system subversion. 25X1

We must be concerned not only with data disclosure, but also with the denial of services at critical times and the alteration of data to make it unreliable and, therefore, unusable. The program outlined above also contains countermeasures addressing these problems. 25X1

Appendix D

Areas Receiving Attention

Current policies and methods for data and communications control, monitoring, and protection attempt to satisfy most of today's requirements. For the most part, they take advantage of currently available technology and incorporate some special features that have been developed within the Agency. 25X1

The following computer security facilities and mandatory security measures exist:

- All users of each Agency system are cleared to the highest classification level of data on that system.
- All equipment including remote terminals and printers is afforded physical protection.
- A limited program for reviewing information systems procurement actions for security implications has been in place for several years.
- A user ID and personal password is assigned to each authorized user of the central computing facilities.
- An exception audit and accounting system records unusual uses of the central systems. These incidents are investigated by Information Systems Security Officers.
- We have begun to build system security awareness by offering information systems security briefings and classes.
- Unlike many computer environments, only a limited number of employees are authorized to modify the software that controls communications and data processing systems.
- Separation of system applications software development and operations in all data processing are being maintained, where practical.
- We have begun an active program of computer center inspections, including external contractor facilities, to determine compliance with established security standards. 25X1

Present mandatory security measures for communications links include the following:

- Error checking routines attempt to ensure data integrity and delivery of data to the proper location.
- All Agency classified data communications links are cryptographically protected with NSA-approved (Class A) cryptographic equipment.
- Audit trails are incorporated into all Office of Communications network switches.
- TEMPEST tests are conducted to certify the integrity of communications security at overseas facilities and aperiodically, as resources allow, at domestic sites.
- The TEMPEST profile of plaintext processing equipment is certified before it is deployed. 25X1

Appendix E

Glossary

End-to-End Encryption. A cryptological application in which protection is afforded to communicated information from one user to another instead of only through part of the transmission path.

Gateway. The functional element that connects two networks. It provides the physical and logical interfaces that will allow information to pass between the networks even if the information is formatted differently in the two networks. The complexity of the gateway can offer opportunities for compromise of data.

Lap-Top Computer. A complete personal computer whose size and packaging enable it to be held in a person's lap, transported in a briefcase, and so forth.

Network. An entity created by the interconnection of hardware elements such as computers, data terminals, and other devices for the purpose of communicating information between multiple devices. In the context of this report, the term means the interconnection of multiple computers in such a way that users who are connected to a specific computer can also access information from other computers in the network.

Retrofit. The process of altering a technical product to conform to design changes that occurred after it was produced.

Trapdoor. A flaw induced in an operating system that when exercised gives the initiator complete logical control of the computer system. A trapdoor is typically a tool for clandestine penetrators to survey and exploit a target system.

Trojan Horse. A program ostensibly providing a user service, such as an operating system, word processing program, spreadsheet program, and so forth, which the attacker can use to introduce his own program. Usually used to attack specific information targets.

Threat. A technical attack or other intentional exploitation of an existing vulnerability in a system.

Volume. A term used for data storage disks.

Vendor Provided. In the context of this paper, vendor-provided products would be fully supported and updated by the company that initially sold them.

Vulnerability. A security flaw or weakness associated with a system's equipment, software, or operations.

This appendix is Unclassified.